DOI 10.52209/1609-1825_2021_4_270 UDC 004.052(942)

Analysis and Research of Reliability Parameters of the Backbone Part of a Multiservice Network Based on Packet Tracer

[1]**MANANKOVA Olga,** *doctoral student, o.manankova@aues.kz,*
[1]**YAKUBOVA Muborak,** *Dr. Tech. Sci., Professor, m.yakubova@aues.kzu,*
[2]***SERIKOV Tansaule,** *PhD, Senior Lecturer, dareka@inbox.ru,*
[1]*Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev, Kazakhstan, 050013, Almaty, A. Baitursynova Street, 126/1,*
[2]*S. Seifullin Kazakh Agrotechnical University, Kazakhstan, 010011, Nur-Sultan, Zhenis Avenue, 62,*
**corresponding author.*

Abstract. *The purpose of the research is to study the influence of the Ping size on the change in the line delay when transmitting information in a multiservice network and the ICMP protocol, in which the reliability parameters cause the equipment to fail. To simulate the hardware and software reliability of a multiservice backbone network, the EIGRP routing protocol and the Ping utility settings based on the Packet Tracer environment were selected. The ICMP protocol and the Ping utility with 32-byte parameters are used as a real-time reliability monitoring tool between two systems in a multi-service network. The obtained results show how the delay value of the transmitted Ping changes and the hardware-software reliability is determined in the developed model. Further, after analyzing the obtained values, as a result of the experiment, the limit of the Ping value is determined, at which the reliability of the secure transmission of information is violated. The conducted studies allow us to assess the state of the equipment at the network level when transmitting information in a multiservice network.*

Keywords: *monitoring, reliability, multiservice network, router, Ping, Packet Tracer, ICMP, EIGRP.*

Introduction

Due to the relevance of the research topic, we will analyze modern foreign and other sources of publications. For example, in [1], a study of the reliability of signal transmission in a multiservice network with the determination of a set of parameters was carried out. The conducted research proves the dependence of reliability on the technical characteristics of the equipment. In the article [2], the characteristics of various routing protocols of a multiservice network are considered, which show a reliable and secure network structure.

In the article [3], the work of the EIGRP and OSPF routing protocols in the IPv4 and IPv6 network topologies is investigated. It is proved that EIGRP has better parameters than OSPF.

The article [4] considers the dynamic routing mode of the EIGRP protocol when using redundant, redundant links and a metric system when designing a backbone corporate network.

In [5], we study the method of building a network using the Packet Tracer program based on the EIGRP routing protocol.

The paper [6] presents a scenario for using the Internet of Things technology to control underwater network devices over the Internet using the new Water Ping protocol, which was based on the ICMP protocol technology, which allows underwater devices to successfully send and receive ping messages.

The article [7] presents an approach to modeling the ICMP Ping Flood attack and analyzing the consequences of an attack on wireless networks using OPNET Modeler.

The article [8] discusses the role and advantages of the packet tracer application software package in the development of computer network construction technology. The ability to explore computer networks without the consciousness of a real network is relevant.

In [9], the method (process) of using the properties of the ICMP protocol as a tool for organizing DDoS attacks on network equipment and an algorithm that uses the specified parameters to detect and prevent the ICMP flood flow is considered.

The simulation carried out in [10] contains the results of an attack on the network using ICMP Ping Flood. The results obtained showed the effect of changes in the size of the attacking packet and the intensity of the attack on the bandwidth of the attacking network.

Based on the analysis of the above sources [1-10], we conclude that the study of the software and

hardware reliability of the backbone of a multiservice network is relevant, and the calculation method based on the change in the Ping value and the study of ICMP attacks in the Packet Tracer environment is the basis of scientific significance.

Configuring a multi-service network on the Packet Tracer environment

The developed multi-service network model consists of devices such as: transmitting part, backbone and adopted part.

Composition of the entire network consist of 11 routers Cisco 2811 series with NM-4A/S expansion card, 2 Switch 2950-24, 6 pcs and 6 servers for different purposes (FTP, DHCP, HTTP).

In the simulation model of the network segment (Figure 1), the main nodes are configured, IP addresses are distributed, and the EIGRP routing protocol is configured, in which LAN1(the transmitting part) is assigned to Area 1, LAN2 (the receiving part) is assigned to Area 2, after which its main performance characteristics are evaluated, consisting of an estimate of the ping delay value over the network through Area 0, which is the backbone part of the network [11].

To test the availability of nodes, a 32-bit Ping of length is set from PC4 in Area 1 with the address 192.168.1.8 to PC2 in Area 2 with the address 192.168.15.5, as shown in Figure 2.

Figure 2 shows that the connection is established, and the loss of transmitted Ethernet packets is "0%". The average round trip time of a packet is 15 ms. This is the best possible result of executing the command. It indicates a small network load and no need to send the same information repeatedly.

Research on the hardware implementation of the security of the trunk part of the multi-service network

Let's take the probability of all routers working as 1, and the probability of each router is calculated based on the ratio of the total number of routers in

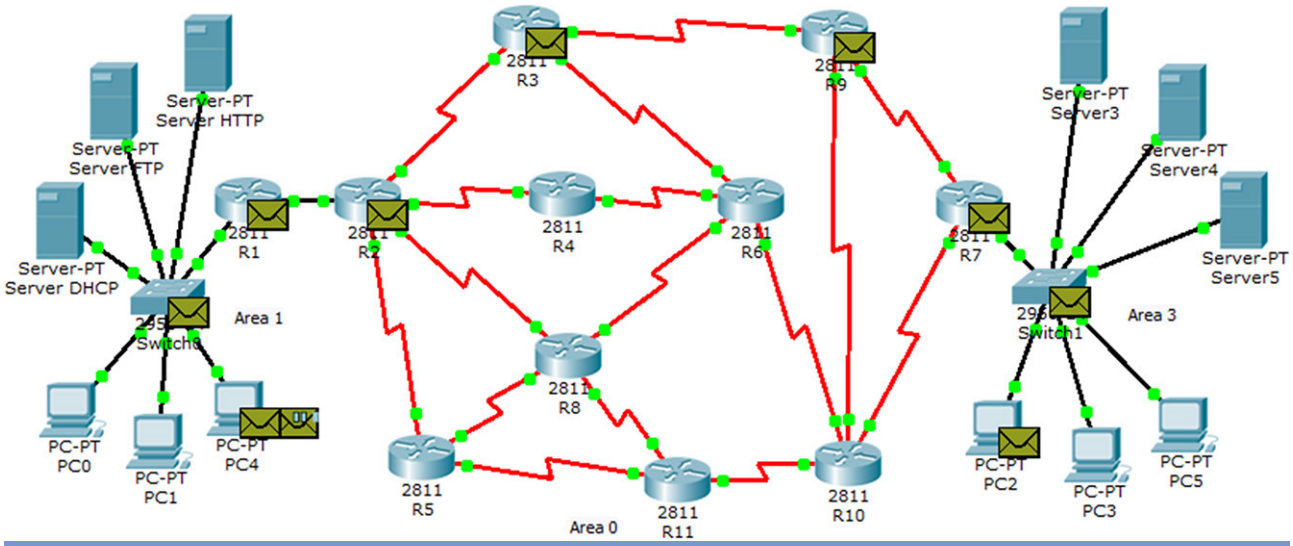

Figure 1 – Network under study

```
PC>ping 192.168.15.5

Pinging 192.168.15.5 with 32 bytes of data:

Reply from 192.168.15.5: bytes=32 time=25ms TTL=123
Reply from 192.168.15.5: bytes=32 time=12ms TTL=123
Reply from 192.168.15.5: bytes=32 time=12ms TTL=123
Reply from 192.168.15.5: bytes=32 time=12ms TTL=123

Ping statistics for 192.168.15.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 25ms, Average = 15ms
```

Figure 2 – The result of passing the Ping

the multiservice network to the total probability. Let's assume that the probability of a single element working is 0.1, given that there are 10 routers in the network.

A study of hardware reliability was carried out when routers were removed from the architecture of the backbone part of the multiservice network in turn. When removing R3, the average delay is 14 ms. Figure 3 shows the result of node availability.

Similarly, measure the delay in the absence of a routers R9, R8, R4. When removing R9, the average delay is 12 ms. When deleting R4, the average delay is 12 ms. When removing R8, the average delay is 11 ms. Figure 4 shows the network after removing the routers.

As a result of the removal of 5 routers that make up 50% of the equipment of the backbone part of the multiservice network, the ping passes to the designated node in 11 ms, which confirms the reliability of the network under study.

Research on the software implementation of the security of the trunk part of the multi-service network

To study the software reliability of the backbone of a multiservice network, an experiment was conducted when the value of pings changed in a large direction when they were transmitted over the network with an interval of 1 ms [12-13], as shown in Table.

Table shows that when the ping value is higher than 15,000 bits, the echo request responses disappear and there is a hardware denial of service.

Conclusion

The study of the backbone part of the multiservice network showed the widespread use of the ICMP protocol and its properties in combination with the EIGRP routing protocol and the modeling technology in the Packet Tracer program.

```
Ping statistics for 192.168.15.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 19ms, Average = 14ms
```

Figure 3 – The result of passing the Ping

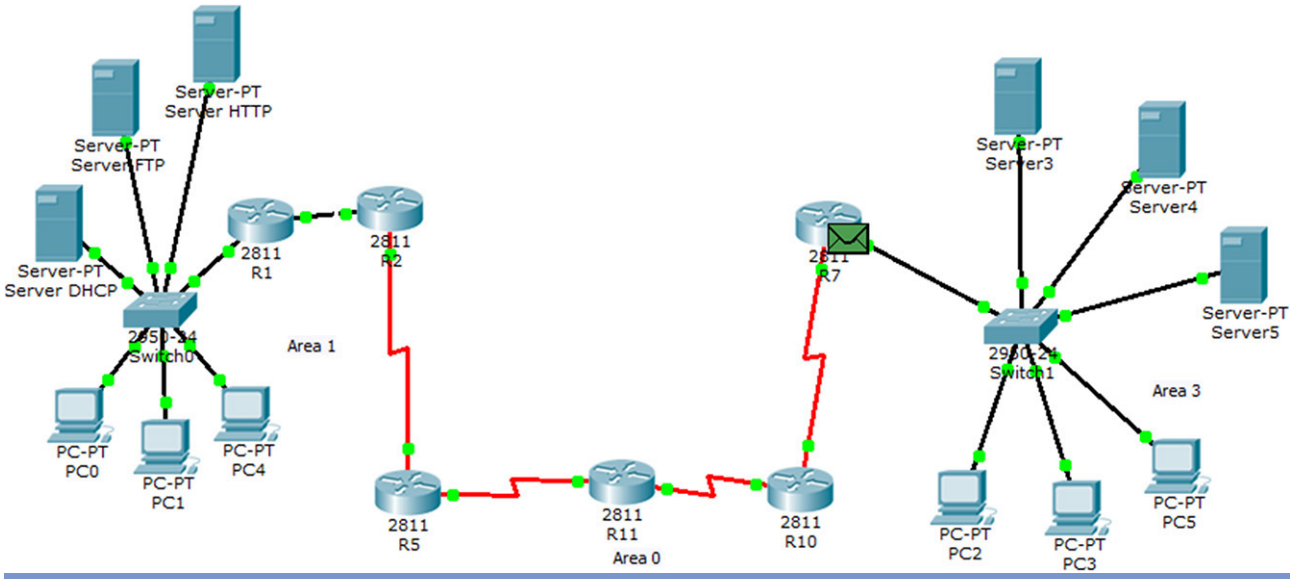

Figure 4 – Multiservice network after the change

Dependence of the delay on the Ping value										
Ping size, bits	32	1024	2048	4096	8192	10000	12000	14000	14500	15000
Delays, ms	17	17	19	21	27	29	31	33	35	Failure of service

The results of the study of the hardware reliability of the backbone of the multiservice network show that the network works reliably with 50% of the availability of equipment and has an average delay of 11 ms.

From the study of software reliability, it can be seen that using the vulnerable sides of the ICMP protocol as the basis for creating an attack on the network in order to disrupt the performance of network equipment, the degree of denial of service of equipment increases with increasing service load. The value at which a complete hardware denial of service occurs is greater than 15,000 bits/ms.

The practical significance of the developed methodology for studying the backbone part of a multiservice network is that the results obtained can be used in the design and modernization of the backbone parts of a multiservice network.

REFERENCES

1. M. Amreyev, B. Yakubov, R. Safin, M. Yakubova. Improving The Quality And Reliability Of Signal Transmission And Reception In Multiservice Networks» News of The National Academy of Sciences of the Republic of Kazakhstan. Physico-mathematical series. ISSN 1991-346X. Volume 2, Number 330 (2020), pp. 75-79, doi.org/10.32014/2020.2518-1726.17.
2. T. Teshabayev, M. Yakubova, T. Nishanbaev, B. Yakubov, T. Golubeva and G. Sadikova. «Analysis and research of capacity, latency and other characteristics of backbone multiservice networks based on simulation modeling using different routing protocols and routers from various manufacturers for using the results when designing and modernization of multiservice networks», 2019 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2019, pp. 1-7, doi: 10.1109/ICISCT47635.2019.9011950.
3. Wijaya, Chandra. (2011). Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network. 10.1109/ICI.2011.64.
4. C.K. Williams, «Tuning Dynamically Routed Internet Protocol Networks to Achieve Controlled and Predictable Failover During Link Instability», MILCOM 2006 – 2006 IEEE Military Communications conference, Washington, DC, 2006, pp. 1-6, doi: 10.1109/MILCOM.2006.302319.
5. P. Srikanth Reddy, P. Saleem Akram, M. Adarsh Sharma, P. Aditya Sai Ram, R. Pruthvi Raj, «Study and Analysis of Routing Protocols», International Journal of Emerging Trends in Engineering Research, Vol 7, No 11, pp. 434-440, 2019 https://doi.org/10.30534/ijeter/2019/067112019.
6. Lima, Francisco & Vieira, Luiz & Vieira, Marcos & Borges, Alex & Miranda Nacif, José. (2019). Water Ping: ICMP for the Internet of Underwater Things. Computer Networks. 152. 10.1016/j.comnet.2019.01.009.
7. Bogdanoski, Mitko & Risteski, Aleksandar. (2011). Wireless Network Behavior under ICMP Ping Flood DoS Attack and Mitigation Techniques. IJCNIS. 3.
8. JAVID, SHEIKH. (2014). Role of Packet Tracer in learning Computer Networks. International Journal of Advanced Research in Computer and Communication Engineering. 3. 2278-1021.
9. Harshita. Detection and Prevention of ICMP Flood DDOS Attack. International Journal of New Technology and Research (IJNTR) ISSN: 2454-4116, Volume-3, Issue-3, March 2017. – Pp. 63-69.
10. Kumar, Ashish & Sharma, Ajay & Singh, Arun. (2012). Performance Evaluation of Centralized Multicasting Network over ICMP Ping Flood for DDoS. International Journal of Computer Applications. 37. 1-6. 10.5120/4641-4361. doi: 10.5120/4641-4361.

Packet Tracer негізінде мультисервистік желі магистралінің сенімділік параметрлерін талдау және зерттеу

*[1]**МАНАНКОВА Ольга Александровна,** докторант, o.manankova@aues.kz,*
*[1]**ЯКУБОВА Муборак Захидовна,** т.ғ.д., профессор, m.yakubova@aues.kz,*
*[2]***СЕРИКОВ Тансауле Габдыманапович,** PhD, аға оқытушы, tansaule_s@mail.ru,*
[1]Ғұмарбек Дәукеев атындағы Алматы энергетика және байланыс университеті, Қазақстан, 050013, Алматы, А. Байтұрсынұлы көшесі, 126/1,
[2]С. Сейфуллин атындағы Қазақ агротехникалық университеті, Қазақстан, 010011, Нұр-Сұлтан, Жеңіс даңғылы, 62,

**автор-корреспондент.*

***Аңдатпа.** Мақалада сенімділік параметрлері жабдықтың істен шығуына әкелетін мультисервистік желіде және ICMP протоколында ақпарат жіберу кезінде желідегі кідірістің өзгеруіне Ping өлшемінің әсері зерттеледі. Packing Tracer бағдарламасын EIGRP маршруттау хаттамасына негізделген және Ping утилитасын конфигурациялаған мультисервистік желі магистралінің аппараттық және бағдарламалық қамтамасыз ету моделін модельдеу үшін пайдалануды көрсетеді. ICMP және 32 байттық Ping мультисервистік желідегі екі жүйе арасындағы нақты уақыт режимін бақылау құралы ретінде қолданылады. Бұл түйіннің бар-жоғын тексеру үшін жеткілікті, бірақ желінің өзі немесе сенімді қосылыстың тұрақтылығын тексеру кезінде жеткіліксіз. Алынған нәтижелер берілген Ping кідірісінің мәні қалай өзгеретінін және дамыған модельде бағдарламалық жасақтама мен аппараттық құралдың сенімділігі қалай анықталатынын көрсетеді. Әрі қарай, алынған мәндерді талдағаннан кейін, тәжірибе нәтижесінде Ping мәнінің шегі анықталады, бұл кезде қауіпсіз*

ақпаратты беру сенімділігі бұзылады. Жүргізілген зерттеулер мультисервистік желіде ақпарат беру кезінде жабдықтың күйін желі деңгейінде бағалауға мүмкіндік береді.

Кілт сөздер: *бақылау, сенімділік, мультисервистік желі, маршрутизатор, Ping, Packet Tracer, ICMP, EIGRP.*

Анализ и исследование параметров надежности магистральной части мультисервисной сети на основе Packet Tracer

[1]***МАНАНКОВА Ольга Александровна,*** *докторант, o.manankova@aues.kz,*
[1]***ЯКУБОВА Муборак Захидовна,*** *д.т.н., профессор, m.yakubova@aues.kz,*
[2]****СЕРИКОВ Тансауле Габдыманапович,*** *PhD, старший преподаватель, tansaule_s@mail.ru,*
[1]*Алматинский университет энергетики и связи им. Гумарбека Даукеева, Казахстан, 050013, Алматы, ул. А. Байтурсынова, 126/1,*
[2]*Казахский агротехнический университет им. С. Сейфуллина, Казахстан, 010011, Нур-Султан, пр. Женис, 62,*
**автор-корреспондент.*

Аннотация. *Цель исследования – изучить влияние размера Ping на изменение задержки в линии при передаче информации в мультисервисной сети и протоколе ICMP, в котором параметры надежности вызывают отказ оборудования. Для моделирования надежности оборудования и программного обеспечения мультисервисной магистральной сети был выбран протокол маршрутизации EIGRP и настройки утилиты Ping на основе среды Packet Tracer. Протокол ICMP и утилита Ping с 32-байтовыми параметрами используются в качестве инструмента мониторинга надежности в реальном времени между двумя системами в мультисервисной сети. Полученные результаты показывают, как изменяется величина задержки передаваемого Ping и определяется аппаратно-программная надежность в разработанной модели. Далее, после анализа полученных значений, в результате эксперимента определяется предел значения Ping, при котором нарушается надежность защищенной передачи информации. Проведенные исследования позволяют оценить состояние оборудования на сетевом уровне при передаче информации в мультисервисной сети.*

Ключевые слова: *мониторинг, надежность, мультисервисная сеть, машрутизатор, Ping, Packet Tracer, ICMP, EIGRP.*

REFERENCES

1. M. Amreyev, B. Yakubov, R. Safin, M. Yakubova. Improving The Quality And Reliability Of Signal Transmission And Reception In Multiservice Networks» News of The National Academy of Sciences of the Republic of Kazakhstan. Physico-mathematical series. ISSN 1991-346X. Volume 2, Number 330 (2020), pp. 75-79, doi.org/10.32014/2020.2518-1726.17.
2. T. Teshabayev, M. Yakubova, T. Nishanbaev, B. Yakubov, T. Golubeva and G. Sadikova. «Analysis and research of capacity, latency and other characteristics of backbone multiservice networks based on simulation modeling using different routing protocols and routers from various manufacturers for using the results when designing and modernization of multiservice networks», 2019 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2019, pp. 1-7, doi: 10.1109/ICISCT47635.2019.9011950.
3. Wijaya, Chandra. (2011). Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network. 10.1109/ICI.2011.64.
4. C.K. Williams, «Tuning Dynamically Routed Internet Protocol Networks to Achieve Controlled and Predictable Failover During Link Instability», MILCOM 2006 – 2006 IEEE Military Communications conference, Washington, DC, 2006, pp. 1-6, doi: 10.1109/MILCOM.2006.302319.
5. P. Srikanth Reddy, P. Saleem Akram, M. Adarsh Sharma, P. Aditya Sai Ram, R. Pruthvi Raj, «Study and Analysis of Routing Protocols», International Journal of Emerging Trends in Engineering Research, Vol 7, No 11, pp. 434-440, 2019 https://doi.org/10.30534/ijeter/2019/067112019.
6. Lima, Francisco & Vieira, Luiz & Vieira, Marcos & Borges, Alex & Miranda Nacif, José. (2019). Water Ping: ICMP for the Internet of Underwater Things. Computer Networks. 152. 10.1016/j.comnet.2019.01.009.
7. Bogdanoski, Mitko & Risteski, Aleksandar. (2011). Wireless Network Behavior under ICMP Ping Flood DoS Attack and Mitigation Techniques. IJCNIS. 3.
8. JAVID, SHEIKH. (2014). Role of Packet Tracer in learning Computer Networks. International Journal of Advanced Research in Computer and Communication Engineering. 3. 2278-1021.
9. Harshita. Detection and Prevention of ICMP Flood DDOS Attack. International Journal of New Technology and Research (IJNTR) ISSN: 2454-4116, Volume-3, Issue-3, March 2017. – Pp. 63-69.
10. Kumar, Ashish & Sharma, Ajay & Singh, Arun. (2012). Performance Evaluation of Centralized Multicasting Network over ICMP Ping Flood for DDoS. International Journal of Computer Applications. 37. 1-6. 10.5120/4641-4361. doi: 10.5120/4641-4361.